主要内容

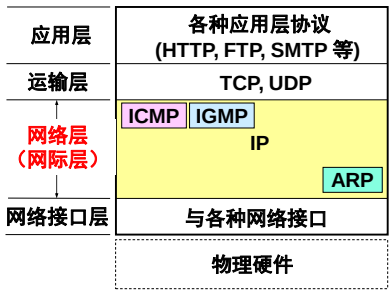
四、网络安全协议

- ◆网络层安全协议 IPSec
  - ❖IPSec VPN的部署
  - ❖IKE基本原理
  - ❖传输模式
  - ❖AH/ESP原理
- ◆传输层安全协议 TLS/SSL

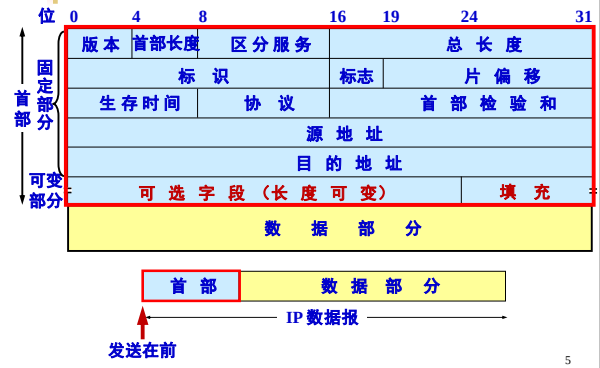
IPSec

网络层的安全协议

Internet的体系结构



IP 分组格式



路由器转发IP分组的算法

(1) 从收到的分组的首部提取目的 IP 地址 D。

(2) 先用各网络的子网掩码和 *D* 逐位相“与”，看是否和相应的网络地址匹配。若匹配，则将分组直接交付。否则就是间接交付，执行 (3)。

(3) 若路由表中有目的地址为 *D* 的特定主机路由，则将分组传送给指明的下一跳路由器；否则，执行 (4)。

(4) 对路由表中的每一行，将子网掩码和 *D* 逐位相“与”。若结果与该行的目的网络地址匹配，则将分组传送给该行指明的下一跳路由器；否则，执行 (5)。

(5) 若路由表中有一个默认路由，则将分组传送给路由表中所指明的默认路由器；否则，执行 (6)。

(6) 报告转发分组出错。

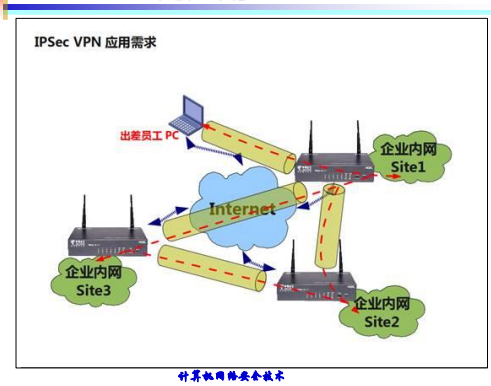
IP协议的安全性问题

- 存在问题
  - 缺乏内置安全措施保证IP分组的真实性和私密性
  - 无法保证IP分组的来源于受信任的源端
  - 没有对IP分组的有效载荷完整性验证
- 解决方法
  - 在网络层提供安全方案：IPSec（Internet Protocol Security）
  - 修改IP协议栈，而不用对网络应用程序进行修改

IP 安全（IP Security）

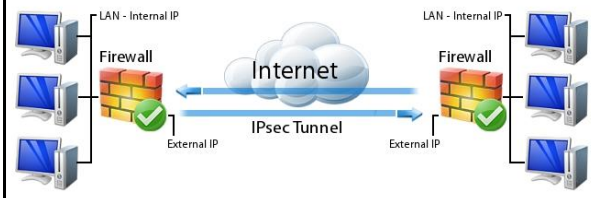
- 1994年，互联网体系结构委员会（IAB）发表“互联网体系结构安全”报告（RFC1636）
  - **下一代IP的安全特性：认证和加密**
  - IPv6实现
- IPSec规范：互联网安全标准
  - IPv4和IPv6中均可使用
- 用途
  - 通用的IP安全机制
  - 认证 authentication
  - 加密 confidentiality
  - 密钥管理 key management

IPSec的应用: IPSec VPN



IPSec VPN的应用场景

- ◆站点到站点或网关到网关（Site-to-Site）
  - ❖例如，一家企业的3个机构分布在互联网的3个不同的地方，各使用一个网关相互建立VPN隧道，企业内网之间的数据通过这些网关建立的IPSec隧道实现安全互联。
- ◆端到端或者PC到PC（End-to-End）
  - ❖ 两个PC之间的通信由两个PC之间的IPSec会话保护
- ◆端到站点或者PC到网关（End-to-Site）
  - ❖两个PC之间的通信由网关和异地PC之间的IPSec进行保护



IPSec 的服务

- ◆通用IP安全机制
  - ❖LAN, WAN, Internet之间，包括以下功能：

数据机密性（Confidentiality）
- ❖ IPsec发送方在通过网络传输包前对包进行加密

数据完整性（Data Integrity）
- ❖ IPsec接收方对发送方发送来的包进行认证，以确保数据在传输过程中没有被篡改

数据来源认证（Data Authentication）
- ❖ IPsec在接收端可以认证发送IPsec报文的发送端是否合法

防重放攻击（Anti-Replay）
- ❖ IPsec接收方可检测并拒绝接收过时或重复的报文

IP Sec体系结构

- ◆ 体系结构
  - ❖ *RFC4301 Security Architecture for Internet Protocol*
- ◆ AH协议
  - 认证报头 Authentication Header (AH)
  - *RFC4302 IP Authentication Header*
- ◆ ESP协议
  - 封装安全负载 Encapsulating Security Payload (ESP)
  - *RFC4303 IP Encapsulating Security Payload (ESP)*
- ◆ IKE协议
  - 密钥管理 Internet Key Exchange (IKE)
  - *RFC7296，8247 Internet Key Exchange (IKEv2) Protocol*
- ◆ 加密算法 Cryptographic algorithms

IPSec体系结构（续）

- RFC2407，*The Internet IP Security Domain of Interpretation for ISAKMP*（1998）
- RFC 2408，*Internet Security Association and Key Management Protocol* (ISAKMP)
- RFC2409，*The Internet Key Exchange* (IKE)
- 其他

IPSec的组成

- Internet密钥交换协议（**IKE:** Internet Key Exchange）
  - 双向交互认证
  - 生成会话密钥
- 封装安全负载和认证报头（ESP/AH）
  - 封装安全负载**ESP**: Encapsulating Security Payload — IP分组加密和完整性保护
    - 通常使用DES、3DES、AES等加密算法实现数据加密，使用MD5或SHA1来实现数据完整性。
  - 认证报头**AH**: Authentication Header — 完整性保护
    - 常用摘要算法（单向Hash函数）：MD5、SHA1
    - 较少使用

IKE
Internet密钥交换协议

Internet密钥交换协议-IKE

- IKE解决了在不安全的网络环境（如Internet）中安全地建立或更新共享密钥的问题
- IKE是一种通用协议，不仅可为IPSec协商安全关联，还可以为SNMPv3、RIPv2、OSPFv2等任何要求保密的协议协商安全参数。
- 由Internet安全关联和密钥管理协议（ISAKMP）和两种密钥交换协议OAKLEY与SKEME组成。
  - IKE创建在由ISAKMP定义的框架上，沿用了OAKLEY的密钥交换模式以及SKEME的共享和密钥更新技术，还定义了它自己的两种密钥交换方式。

说明：ISAKMP/Oakley

- Oakley Key Determination Protocol
  - 基于DH（Diffie-Hellman）算法的密钥交换协议，并增强安全性
- Internet Security Association and Key Management Protocol (ISAKMP)
  - Internet密钥管理框架，支持多种特定协议，包括格式及安全属性协商
  - 消息集合
- 在IKEv2中，不再使用这两个术语，但基本功能是相同的。

两个版本：IKEv1和IKEv2

- IKEv1版本分两个阶段动态建立IPSec SA
  - 阶段1-建立IKE SA：阶段1采用主模式或积极模式协商。
  - 阶段2-建立IPSec SA：阶段2此采用快速模式协商。
  - 预共享密钥是最简单、最常用的身份认证方法。这种方式下设备的身份信息可以用IP地址或名称来标识。
- IKEv2
  - 协商建立IPSec SA的速度大大提升
  - 增加了EAP（Extensible Authentication Protocol）方式的身份认证。
    - 解决了远程接入用户认证的问题，彻底摆脱了L2TP的牵制
    - 目前IKEv2已经广泛应用于远程接入网络中了。

Internet密钥交换协议-IKE

- 提供双向交互认证和会话密钥
  - 复杂性：大量内置选项和技术特性
- IKE使用了两个阶段的ISAKMP
  - **阶段 1** — IKE安全关联 security association (IKE-SA)
    - 通信各方彼此间建立了一个已通过**身份认证**和安全保护的通道
    - **“建立会话”**
  - **阶段 2** — AH/ESP安全关联 security association (IPSec-SA)
    - 用在第一阶段建立的安全隧道为IPsec协商安全服务，即为IPsec协商具体的SA，建立用于最终的IP数据安全传输的IPsec SA
    - **“建立连接”**

IKE 阶段1的主要工作

- 进行IPSec对等体（peer）的身份认证
- 在对等体之间协商能匹配的IKE SA策略，以保护IKE密钥交换
- 使用Diffie-Hellman算法生成共享密钥
- 建立安全隧道，用于协商IKE第2阶段参数

IKE 阶段 1

◆IKE中有4种身份认证方式

（1） 基于公开密钥（Public Key Encryption），利用对方的公开密钥加密身份，通过检查对方发来的该HASH值作认证。

（2） 基于修正的公开密钥（Revised Public Key Encryption），对上述方式进行修正。

（3） 基于数字签名（Digital Signature），利用数字证书来表示身份，利用数字签名算法计算出一个签名来验证身份。

（4） 基于预共享密钥（Pre Shared Key），双方事先通过某种方式商定好一个双方共享的字符串。

阶段1的两种工作模式

◆主模式 Main mode

- ❖在对等体间进行三次双向交换（由6条消息组成），协商匹配对等体间的IKE SA值
  - ➢第1次交换：协商用于保护IKE通信的哈希算法，确保每个对等体的IKE SA策略能够匹配一致；
  - ➢第2次交换：使用Diffie-Hellman算法生成对等体之间的共享密钥
  - ➢第3次交换：验证对等体身份，其中身份信息是加密形式的对等体IP地址。

◆积极模式（野蛮模式） aggressive mode

- ❖仅进行一次双向交换，对等体双方都将协商所需的一切（如：DH公钥、身份信息等）放在IKE SA中，一次性的发送给对端。

IKE 阶段1

◆IKE 阶段1有8个不同的版本，主要有6个变体

- ❖公开密钥签名 (main & aggressive modes)
- ❖对称密钥加密 (main and aggressive modes)
- ❖公开密钥加密 (main and aggressive)

◆为什么需要公钥签名和公钥加密?

- ❖公钥签名
  - ➢每个人都知道自己的私有密钥
  - ➢**初始时可能不知道对方的公开密钥**
  - ➢数字签名方式：执行协议启动过程，查找对方公钥（提高效率）
- ❖公钥加密
  - ➢需要知道对方的公钥

回顾：Diffie-Hellman算法

◆假定p 为素数, g 为生成器 **generator** （本原根）

- ❖ For any $x \in \{1,2,\ldots,p-1\}$ there is n s.t. $x = g^n \bmod p$

◆Alice 随机选择秘密指数 a

◆Bob 随机选择秘密指数 b

◆Alice 向Bob发送 $g^a \bmod p$

◆Bob 向Aliace 发送 $g^b \bmod p$

◆**双方计算共享密钥 $g^{ab} \bmod p$**

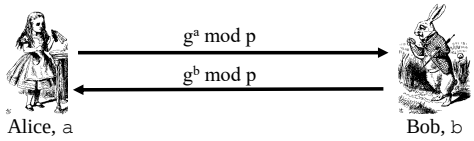
◆该密钥可作为**对称密钥 symmetric key**

D-H算法的安全性

- ❖ 必须使用非常大的*a*, *b* 以及 *p*，从*g*, *p*和$g^a \bmod p$ 中很难计算出 *a*

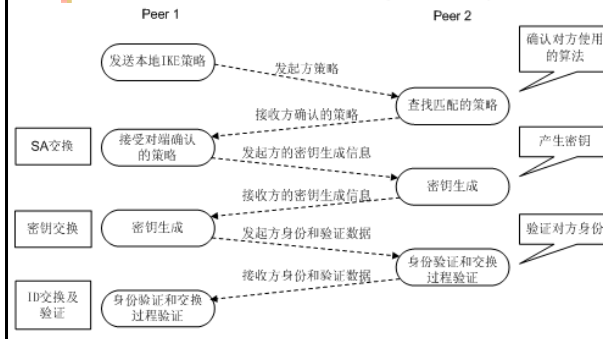
回顾：Diffie-Hellman算法

- DH算法依赖于离散对数计算复杂性
- 公开的: 素数 p和生成器g
- 私有的: Alice的协商指数 a, Bob的协商指数 b

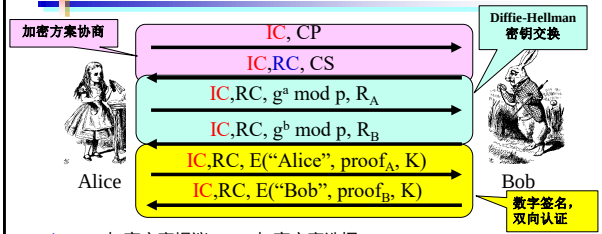


- **Alice计算 $(g^b)^a = g^{ba} = g^{ab}$ mod p**
- **Bob 计算 $(g^a)^b = g^{ab}$ mod p**
- **使用 $K = g^{ab}$ mod p 作为对称密钥**

IKE 阶段 1: 数字签名（主模式）-1



IKE 阶段 1: 数字签名（主模式）

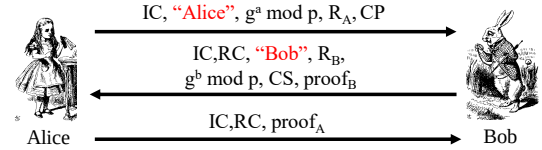


- CP = 加密方案提议, CS = 加密方案选择
- IC = 发起方"cookie", RC = 响应方 "cookie" 抗阻塞令牌
- K = h(IC, RC, g^{ab} mod p, R_A, R_B)
- SKEYID = h(R_A, R_B, g^{ab} mod p)
- $proof_A$ = [h(SKEYID,g^a mod p,g^b mod p,IC,RC,CP,"Alice")]$_{Alice}$

h（）：哈希运算
R_A, R_B：Nonce值，随机数

Alice签名

IKE 阶段 1: 数字签名（积极模式）-2

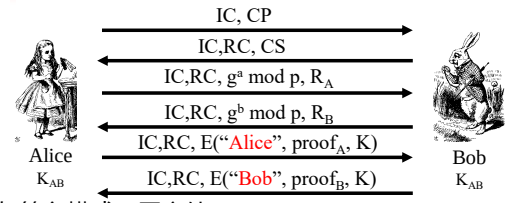


- 与主模式的区别
  - 主模式：提供匿名特性
  - 积极模式：不需要保护通信双方的身份标识；直接发送DH值
  - 简化协议的交互过程

主模式 vs 积极模式

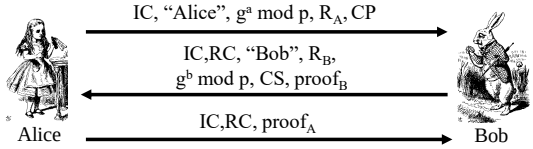
- 主模式必须MUST实现
- 积极模式应该 **SHOULD** 实现
- 互操作问题
- 用公开密钥进行签名和认证
  - **被动攻击者Passive attacker在积极模式中可以知道Alice和Bob的标识ID，而在主模式中不能**
  - **主动攻击者Active attacker在主模式中能够推断Alice和Bob的标识ID**

IKE 阶段 1: 对称密钥（主模式） -3



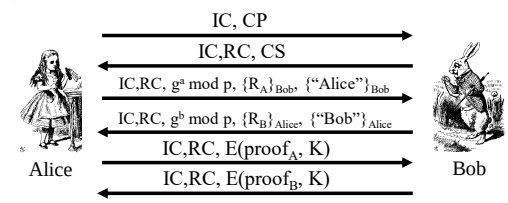
- 与签名模式不同之处
  - K_{AB} = 预先共享的对称密钥
  - K = h(IC, RC, g^{ab} mod p, R_A, R_B, K_{AB})
  - SKEYID = h(K, g^{ab} mod p) 会话密钥
  - $proof_A$ = h(SKEYID,g^a mod p,g^b mod p,IC,RC,CP,"Alice")

IKE 阶段 1: 对称密钥 (积极模式) -4



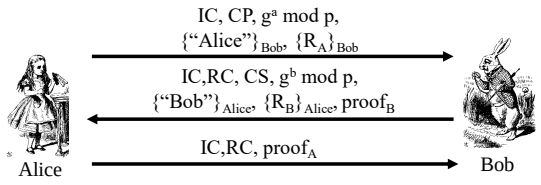
- 表示方法与数字签名选项下的积极模式相同
- 密钥和签名的计算方法与对称密钥选项下的主模式情况相同
- 没有隐藏通信方的身份

IKE 阶段1: 公开密钥加密方式 (主模式) -5



- CP =加密方案提议, CS =加密方案选择
- IC = 发起方 "cookie", RC = 响应方 "cookie"
- K = h(IC,RC,g^{ab} mod p,R_A,R_B)
- SKEYID = h(R_A, R_B, g^{ab} mod p)
- $proof_A$ = h(SKEYID,g^a mod p,g^b mod p,IC,RC,CP,"Alice")

IKE 阶段1:公开密钥加密方式 (积极模式) -6



- K, $proof_A$, $proof_B$ 的计算与主模式相同
- 隐藏身份

IKE 阶段 1 Cookies

- IC 和RC — cookies
  - 抗阻塞令牌(anti-clogging tokens)，防止拒绝服务（DoS）攻击
  - RFC建议将源、目IP，源、目端口，本地生成的随机数,日期和时间进行hash操作，生成cookie值
- 为降低 DoS 攻击的危险，通信双方尽可能保持无状态（**stateless**）方式
  - 如TCP SYN flooding
- 存在问题
  - Bob必须从第1条消息开始记录加密方案提议CP（在第6条消息中要用到）
- 实际上，Bob必须保持状态（从第1条消息开始）
  - 仍存在 DoS 攻击的风险

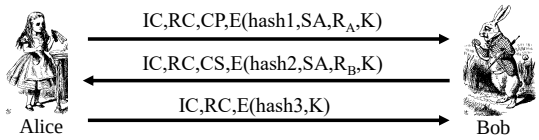
IKE 阶段1 总结

- IKE 阶段 1 的结果
  - 双向交互身份认证
  - 建立共享的会话密钥
  - IKE-SA安全关联 (**Security Association, SA)**
- 但是，阶段1的开销较高
  - 特别是公开密钥与主模式
- IKE阶段2
  - IPSec-AS安全关联

阶段2的工作模式

- **快速模式（Quick mode）：** 在阶段1建立了安全隧道后，进入快速模式
  - 协商共享的安全策略，产生用于IPSec安全算法的共享密钥，建立IPSec SA。
  - 每个对等体在协商后，至少会产生**两个单向的IPSec SA**（一个入站和一个出站）。

IKE 阶段 2



- 会话密钥 K, IC, RC 和 SA 与阶段1相同
  (SA为阶段1建立的IKE-SA标识符)
- 加密方案提议CP 包括ESP and/or AH
- Hashes 1,2,3 依赖于 SKEYID, SA, R_A and R_B （ R_A 和R_B 与阶段1中不同）
- 密钥生成 KEYMAT = h(SKEYID,R_A,R_B,junk)，junk为公开值
- SKEYID依赖于阶段1的密钥方案
- 可选项：PFS (ephemeral Diffie-Hellman exchange)

小结：IPsec与IKE的关系

- IKE是UDP 之上的一个应用层协议，是IPsec的信令协议；
  - 源和目标都是使用的UDP 500
- IKE为IPsec协商建立SA，并把建立的参数及生成的密钥交给IPsec；
- IPsec使用IKE建立的SA对IP报文加密或认证处理。
- IPsec使用AH或ESP报文头中的序列号实现防重放。此序列号是一个32比特的值，此数溢出后，为实现防重放，SA需要重新建立，这个过程需要IKE协议的配合
- IPsec的大规模使用，必须有CA（Certificate Authority，认证中心）或其他集中管理身份数据的机构的参与
- IKE提供端与端之间动态认证。

IKE的安全性

- IKE的加密算法强度高，密钥长度大
  - IKE共定义了五个DH组，其中三个组使用乘幂算法（模数位数分别是768、1024、1680位），另两个组使用椭圆曲线算法（字段长度分别是155、185位）
- 完整性保护及身份验证
  - 在阶段1、2交换中，IKE通过交换验证载荷（包含散列值或数字签名）保护交换消息的完整性，并提供对数据源的身份验证。
- 抵抗拒绝服务攻击
  - 使用Cookie，提供了一定程度的抗拒绝服务攻击的能力
- 防止中间人攻击

SA的建立方式

- 手工方式（manual）
  - 配置比较复杂，创建SA所需的全部信息都必须手工配置，而且不支持一些高级特性（例如定时更新密钥），但优点是可以不依赖IKE而单独实现IPsec功能。
  - 小型静态环境，与之进行通信的对等体设备数量较少
- IKE自动协商（isakmp）
  - 配置好IKE协商安全策略的信息，由IKE自动协商来创建和维护SA。
  - 中、大型的动态网络环境中，推荐使用IKE协商建立SA。

安全关联（Security Associations）

- 也称为安全联盟
- 发送方和接收方之间的提供流量安全性 的单向关系
- 三个参数:
  - 安全参数索引 (Security Parameter Index，SPI)
    - SPI：唯一标识SA的一个32比特数值，它在AH和ESP头中传输
    - 在手工配置SA时，需要手工指定SPI的取值
    - 使用IKE协商产生SA时，SPI将随机生成
  - IP 目的地址
  - 安全协议标识（AH或ESP）
- 具有其他参数
  - 序号， AH信息，ESP信息，生命期等
- 拥有一个安全关联数据库SAD

SA的生存周期

- IKE协商建立的SA的生存周期有两种定义方式
  - 基于时间的生存周期，定义了一个SA从建立到失效的时间；
  - 基于流量的生存周期，定义了一个SA允许处理的最大流量（字节计数）。
- 生存周期到达指定的时间或指定的流量，SA就会失效。
- SA失效前，IKE将为IPsec协商建立新的SA

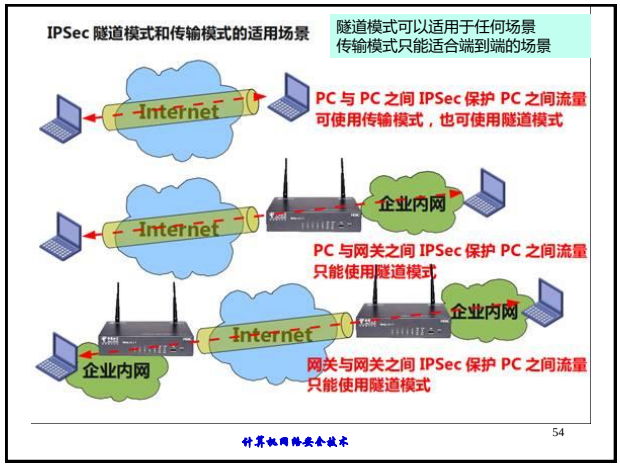
安全策略数据库

- 将IP traffic关联到特定的SAs
  - 将IP流量的子集匹配到相关的SA
  - 使用选择器过滤输出流，以便映射到特定SAs
  - 基于：本地或远程地址，下层协议，名称，本地或远程端口

Protocol	Local IP	Port	Remote IP	Port	Action	Comment
UDP	1.2.3.101	500	*	500	BYPASS	IKE
ICMP	1.2.3.101	*	*	*	BYPASS	Error messages
*	1.2.3.101	*	1.2.3.0/24	*	PROTECT: ESP intransport-mode	Encrypt intranet traffic
TCP	1.2.3.101	*	1.2.4.10	80	PROTECT: ESP intransport-mode	Encrypt to server
TCP	1.2.3.101	*	1.2.4.10	443	BYPASS	TLS: avoid double encryption
*	1.2.3.101	*	1.2.4.0/24	*	DISCARD	Others in DMZ
*	1.2.3.101	*	*	*	BYPASS	Internet

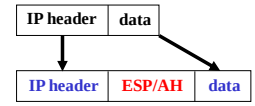
IPSec提供的两种封装模式

- 传输Transport模式
  - 原始IP头部保持不变，主要用于端到端（主机PC到主机PC）的应用场景。
- 隧道Tunnel模式
  - 封装了一个外网IP头，主要用于站点到站点（Site-to-Site）的应用场景。



IPSec 传输模式

◆IPSec 传输模式



◆用于*主机到主机* 通信

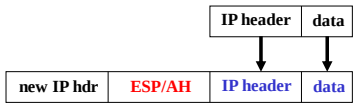
◆高效：仅增加少量额外头部信息

◆保持原始IP头部

- ❖ 安全性
  - ➢ 被动攻击者可以发现通信双方的地址

IPSec 隧道模式

◆IPSec隧道模式 Tunnel Mode



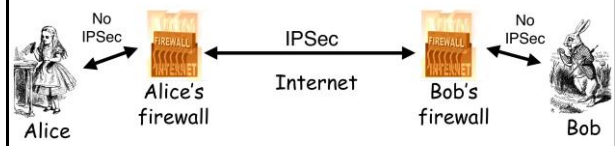
◆用于*站点之间*的通信

- ❖ 原始IP分组被封装在IPSec中

◆原始IP头部对攻击者不可见

例：IPSec部署在防火墙上

◆IPSec 隧道模式



IPSec 的两个协议：ESP/AH

- 保护类型
  - 保密 Confidentiality?
  - 完整性Integrity?
  - 二者兼备?
- 保护对象
  - 数据？分组头部?
  - 二者兼备?

- AH(Authentication Header)
  - 数据完整性保护，不支持加密
- ESP(Encapsulating Security Payload)
  - 数据完整性和保密性

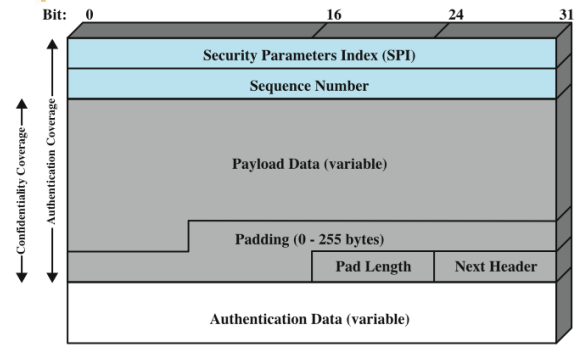
AH协议

- IP协议号为51
- 提供数据源认证、数据完整性校验和防报文重放功能
- 它能保护通信免受篡改，但不能防止窃听，适合用于传输非机密数据。
- 工作原理
  - 在每一个数据包上添加一个身份验证报文头，此报文头插在标准IP包头后面，对数据提供完整性保护
  - 可选择的认证算法有MD5（Message Digest）、SHA-1（Secure Hash Algorithm）等。

ESP协议

- IP协议号为50
- 提供加密、数据源认证、数据完整性校验和防报文重放功能。
- 工作原理
  - 在每一个数据包的标准IP包头后面添加一个ESP报文头，并在数据包后面追加一个ESP尾。
  - 与AH协议不同的是，ESP将需要保护的用户数据进行加密后再封装到IP包中，以保证数据的机密性。
  - 常见的加密算法有DES、3DES、AES等。同时，作为可选项，用户可以选择MD5、SHA-1算法保证报文的完整性和真实性。
  - 空加密NULL encryption

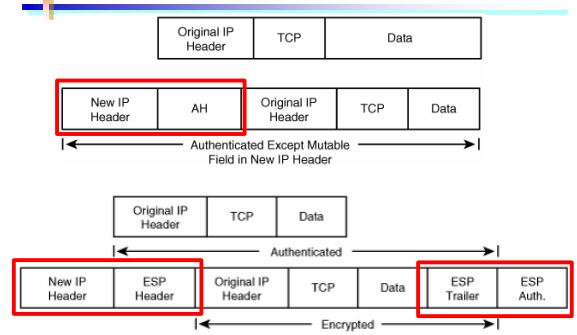
Encapsulating Security Payload (ESP)



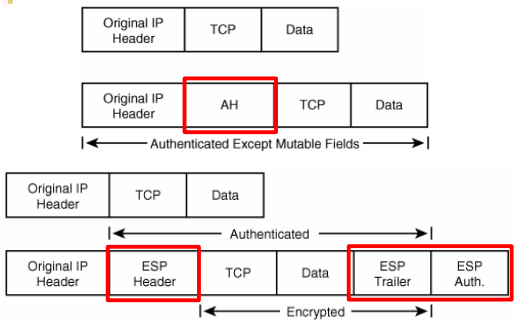
说明：加密 & 认证算法 & 填充

- ESP 能够加密负载数据，填充域、填充长度和邻接报头域
  - 如果使用密码同步数据，初始向量IV可以放在负载数据的开始处
- ESP可以支持可选的ICV完整性校验值
  - 在加密完成后进行计算
- ESP 使用填充
  - 扩充明文到所需要的长度
  - 对齐填充长度和邻接报文头域，32bit的字
  - 提供部分流量的保密

AH/ESP的隧道模式



AH/ESP的传输模式



IPSec实现：加密卡

- IPsec在设备上的实现
  - 通过软件实现：由于复杂的加密/解密、认证算法会占用大量的CPU资源，从而影响设备整体处理效率
  - 通过加密卡实现：复杂的算法处理在硬件上进行，从而提高了设备的处理效率。
- 加密卡进行加/解密处理的过程
  - 设备将需要加/解密处理的数据发给加密卡，加密卡对数据进行处理，然后加密卡将处理后的数据发送回设备，再由设备进行转发处理。

IPSec的优点

- 支持IKE（Internet Key Exchange，因特网密钥交换）
  - 实现密钥的自动协商功能，减少了密钥协商的开销
  - 可以通过IKE建立和维护安全关联（SA）的服务，简化IPsec的使用和管理
- 应用透明性
  - 所有使用IP协议进行数据传输的应用系统和服务都可以使用IPsec，而不必对这些应用系统和服务本身做任何修改
  - 对端用户透明
- 可以对个人用户提供安全性

IPSec的优点(续)

- 数据的加密是以数据包为单位
  - 灵活性，可以有效防范网络攻击
  - 防止被旁路
- 提供安全路由体系结构
  - 路由器广播来源于授权的路由器
  - 相邻路由器广播来源于授权路由器
  - 重定向报文：来自发出初始包的路由器
  - 路由更新未被伪造

IPSec 局限性

- 通信性能较低
- 需要为每一客户端安装客户端软件,可能带来了与其他系统软件之间兼容性问题的风险
- 安装和维护困难
- 不易解决网络地址转换(NAT)和“穿透”防火墙的问题。

IPSec的复杂性

- IPSec 运行在网络层，不能从用户空间直接访问。
  - 支持数据加密，数据完整性保护及身份认证
- 主要用于虚拟专用网**VPN**
- IPv6的基本要求之一
- 过度设计（**Over-engineered**）
  - 协议的复杂性；缺陷；互操作性
- IPsec协议不是一个单独的协议，它给出了应用于IP层上网络数据安全的一整套体系结构

传输层安全 -SSL/TLS

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

Web 安全需求

- WWW的广泛应用
  - 客户/服务器应用
  - 双向通信；门户和信息出口；软件复杂性；用户的多样性
- Web的安全威胁
  - 完整性 integrity: 木马，消息篡改等
  - 保密性 confidentiality：窃听
  - 拒绝服务 denial of service：DDOS, DOS攻击
  - 认证 authentication：假冒合法用户
- 需要增加安全机制
  - Web服务器
  - 浏览器
  - 浏览器和服务器之间的网络通信